Utah Technical Architecture
Production Data Storage Policy
March 21, 2002

Title: Production Data Storage Policy

Introduction: Production data constitutes one of the most valuable information resources that belong to the State of Utah. Lack of access to production data can cause inconvenience and in many instances irreparable harm to the State. Such data must be protected physically and electronically, and provision must be made for recovery in the event of a disaster or cyber attack on the States information resources.

Purpose: This policy sets minimum standards for data accessed by all State information systems that are considered to be in a production environment.

Application: All state agencies of the executive branch of government shall comply with this policy, which shall apply to all computer systems used to host production data.

Definition: The following terms and definitions are used within this policy document:

Agency Specific Storage Resources: **Agency specific storage resources are those that meet the needs of a specific line of business within an agency or a specific agency within a department.**

Availability: the time, during which a mission critical system is working without failure, commonly referred to as uptime. **Mission critical** State systems are expected to be available on a 24 X 7 basis with 99% or greater availability.

Backup Data: Additional resources or duplicate copies of data on different storage media for emergency purposes.

Disaster Recovery: A plan for duplicating computer operations after a catastrophe occurs, such as a fire or earthquake. It includes routine off-site backup as well as a procedure for activating necessary information systems in a new location.

Enterprise Storage Resources: **Enterprise storage resources are those that meet the needs of multiple agencies or multiple lines of business within a department or multiple departments within state government.**

Minimum Physical Facility Requirements: **Mission critical** production data should be stored in a physical facility that provides a controlled temperature environment, redundant backup power, automated fire suppression, server monitoring and reporting, and restricted access controls compliant with Federal Guidelines for C2 security compliance.

Mission Critical: Any production information system that is vital to the operation of an agency or to the State enterprise.

Physical Security: The protection of server environments from unauthorized physical access.

Production Data: A ~~**central**~~ database ~~**or service**~~ containing an organization's master files and daily transaction files running on a computer system used to process an organization's daily work.

Reliability: The speed with which a system can recover from a failure in a high availability production environment.

Authority: *Utah Code Section 63D Information Technology Act*.

Policy: It is the policy of the State of Utah that:

1) All **mission critical** production servers and associated data are housed in a physically secure environment with access controls that do not permit unauthorized users to gain physical access to production data or server environments.

2) All production data will be backed up on a regular basis as required by the data and application owner, and that such backups be stored ~~at~~ off-site ~~data centers such as the Richfield Data Center~~.

3) All production data environments will be protected from electronic security intrusions by a ~~**tiered**~~ firewall implementation with approved intrusion detection capabilities ~~**for each tier**~~. **Such firewall and intrusion detection implementation will be tiered, when required by the data or the application owners.**

4) All **mission critical** production data will be stored using enterprise storage resources in preference to agency specific storage **resources** ~~environments~~ to ensure redundant storage of data and consistent disaster recovery data storage.

5) Agencies that wish to handle ~~all~~ production data storage without using enterprise storage resources may do so with specific permission from the CIO~~, if all other minimum physical facility requirements and disaster recovery are fully satisfied~~.

6) All **mission critical** production data will meet current State availability requirements.

7) Regardless of enterprise or agency specific, all storage resources for mission critical production data must be stored in a physical facility that provides a controlled temperature environment, redundant backup power, automated fire suppression, server monitoring and reporting, and restricted access controls compliant with Federal Guidelines for C2 security compliance.

8) Agencies that wish to use "Agency Specific Storage Resources" for applications deployed after 7/1/2002, may do so only with specific permission from the CIO.

Procedures: For mission critical applications deployed before July 1, 2002 and which do not meet requirements 1 through 3 of this policy, the agency must provide a plan to the CIO by June 30, 2002 to become compliant. For mission critical applications deployed after July 1, 2002 or for existing enterprise storage resources that need to be extended to meet enterprise or agency-specific storage resource needs, the agency must work with the Division of Information Technology Services (ITS) to develop appropriate storage service levels for production data hosting, availability, security, and disaster recovery. Consideration will be given to use existing agency specific storage resources as appropriate. Such plans shall be submitted to the CIO through the IT Planning process. ~~Agencies are directed to identify all agency production data, and work with the Division of Information technology Services (ITS) to develop appropriate storage service levels for production data hosting, availability, security, and disaster recovery. Consideration will be given to use existing agency data resources as appropriate. Such plans shall be submitted to the CIO not later than June 30, 2002 and will thereafter be updated on an annual basis.~~

Exceptions: Data and server environments that are used only for development and testing are excluded from the provisions of this policy.

Impacts: Agencies may wish to collocate their production data servers in the Salt Lake City and Richfield data centers. System administration and data base administration services related to production data resources are provided at rates approved by the Rate Committee.

Review Cycle: This policy will be reviewed on an annual basis.

References:

State Information Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Final Presentation Date: March 28, 2002
Related Policies and Documents: *Security Executive Order, State Information Security Policy; NIST Security Self-Assessment Guide.*
Review Cycle: Annual